Electronic Signatures

Action items for electronic transactions:
Identification / Authentication / Authorization / Intent

presented by:
Office of the Secretary of State
Michael Totherow, Chief Information Officer
Russ Savage, Electronic Transactions Liaison

Establishing a collaborative business requirements framework for

Directory Enabled Networking (DEN),

Smart Devices,

Policy Based Authorization, and

Electronic Signatures

Connecting the dots

Linking

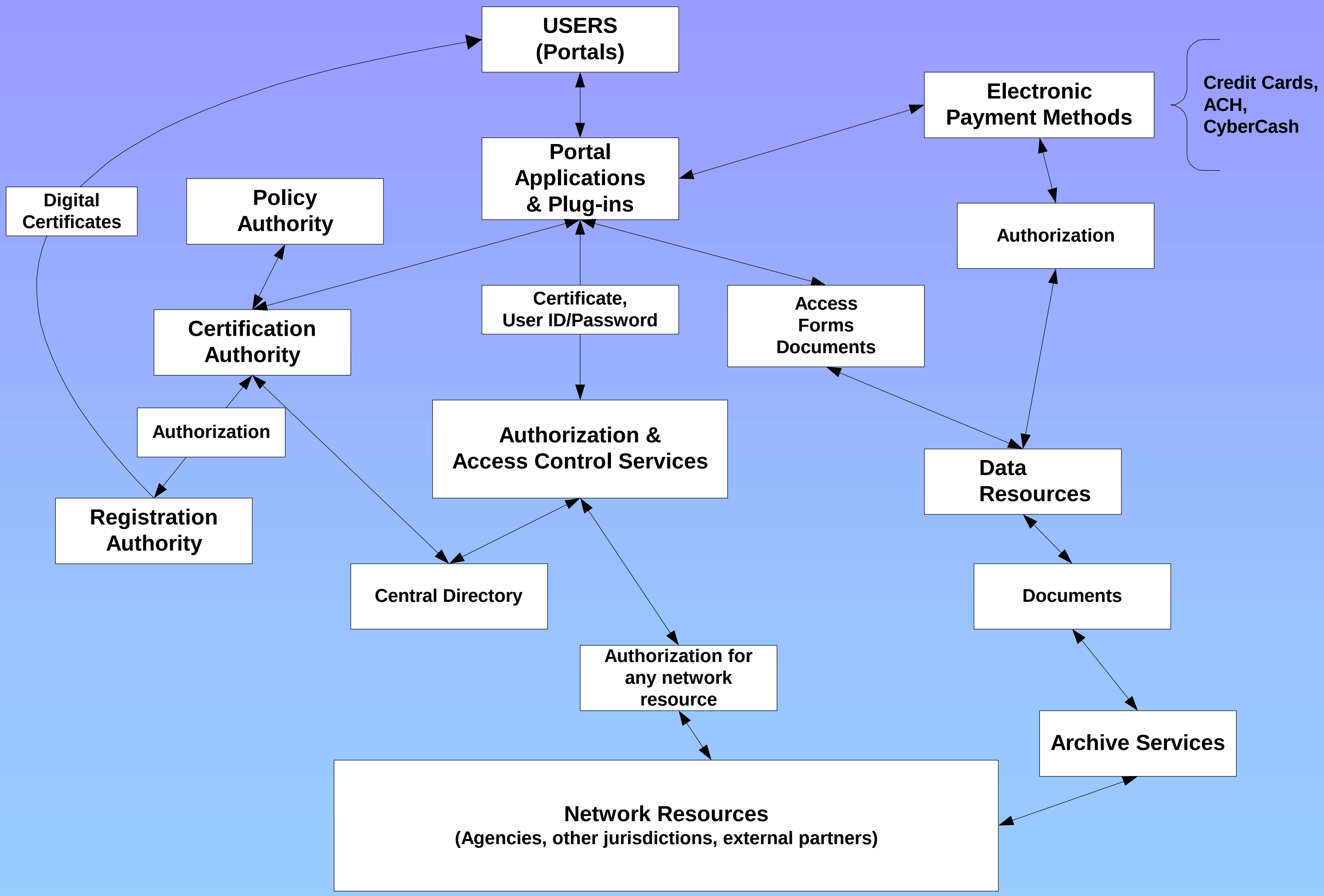
1) Electronic Signatures,

2) electronic records life cycle, and
3) online transactions to the need to identify, authenticate & authorize parties.

Proposed bridge between managing the parties & managing the transactions

Implications for Directory Services and network management

E-government Architectural Framework



Arizona Statute 41-132 establishes the *lawful use of electronic signatures by and with state agencies*.

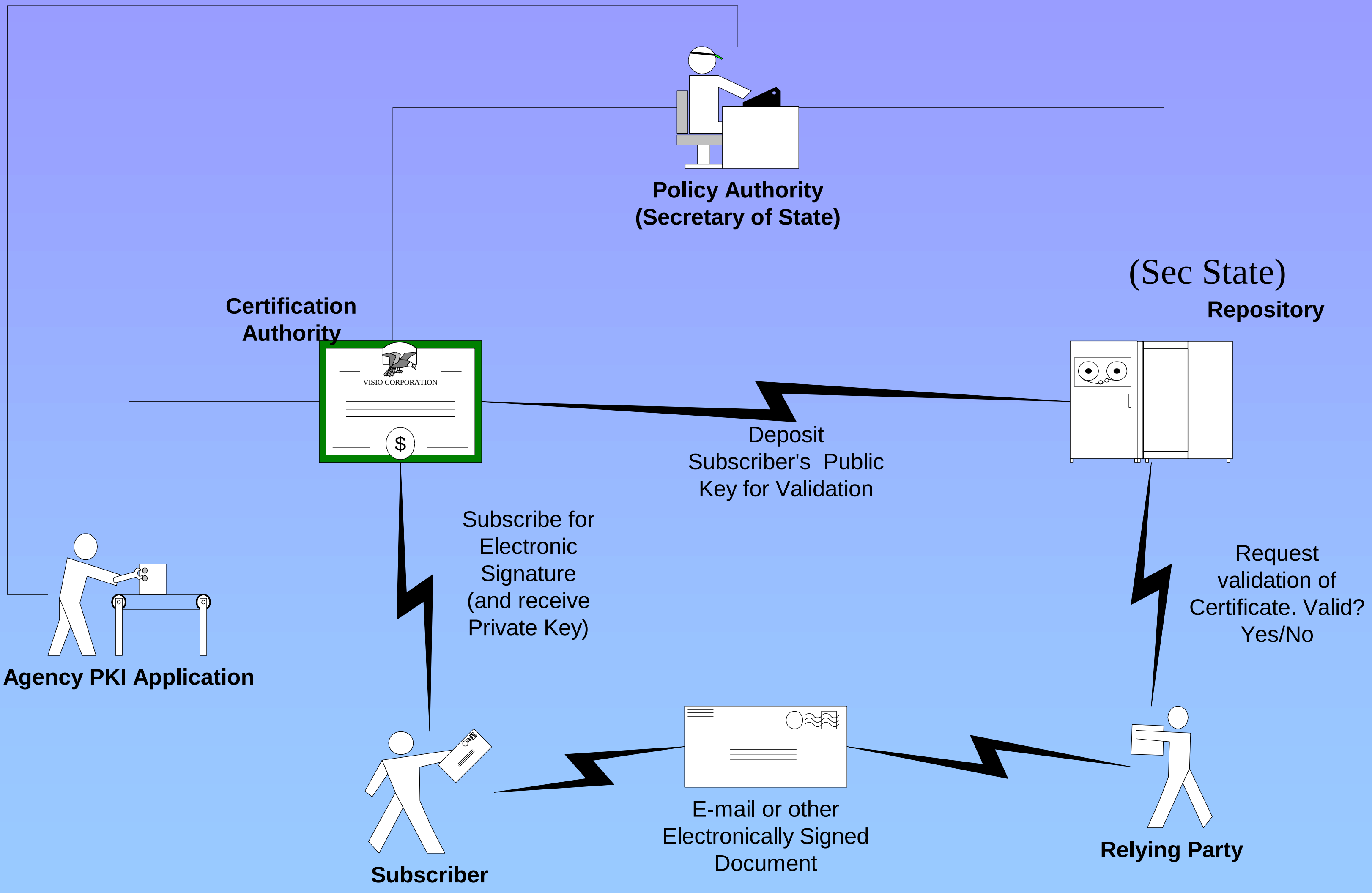
An electronic signature

- shall be unique to the person using it,
- shall be capable of reliable verification and
- shall be linked to a record in a manner so that
  if the record is changed
  the electronic signature is invalidated.

The Secretary of State is responsible for establishing the *legal and business process framework* for the implementation of the statute. Administrative rules for this statute:

- establish the Secretary of State as Policy Authority
- GITA as reference for technical standards

The Roles in Electronic Signature Use



Policy Authority
(Secretary of State)

Certification
Authority

(Sec State)
Repository

Deposit
Subscriber's Public
Key for Validation

Subscribe for
Electronic
Signature
(and receive
Private Key)

Request
validation of
Certificate. Valid?
Yes/No

Agency PKI Application

Subscriber

E-mail or other
Electronically Signed
Document

Relying Party

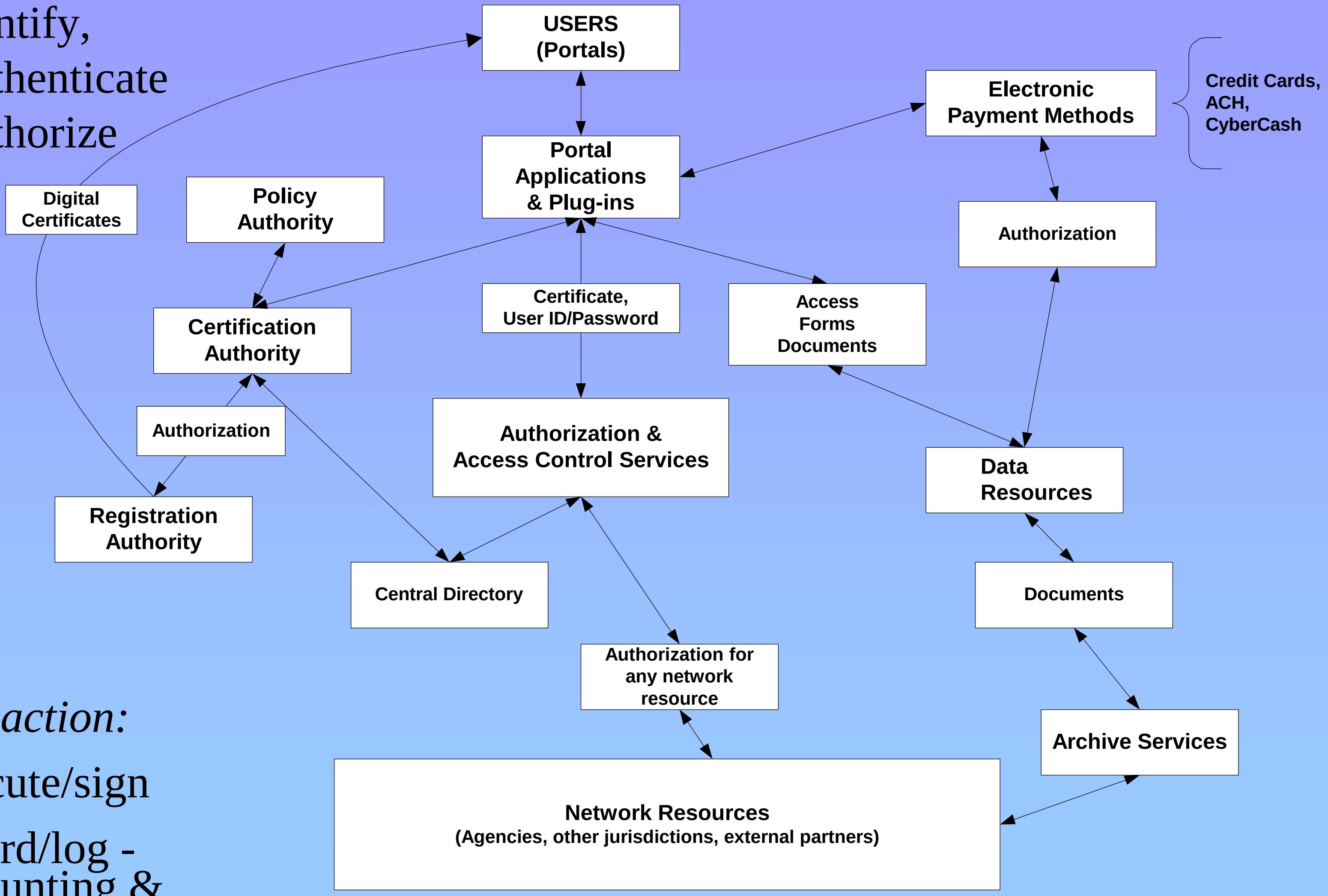
- Electronic signature - signed electronic government records are electronic public records
- Credit/payment card use and electronic notarial acts also create electronic public records.
- It is estimated that about one third of all business documents (public records) are formed and kept in an organization's messaging system (email and word processing).
- The passage of Arizona's Electronic Signature Act, AETA and the federal E-SIGN Act all create a *business need* to define and implement methods for *managing electronic government records* that will remain electronic throughout their life cycle.

Online transactions - portal or otherwise

E-government Architectural Framework

User:

- Identify,
- Authenticate
- Authorize


USERS (Portals)
Electronic Payment Methods
Credit Cards, ACH, CyberCash
Portal Applications & Plug-ins
Digital Certificates
Policy Authority
Authorization
Certificate, User ID/Password
Access Forms Documents
Certification Authority
Authorization
Authorization & Access Control Services
Data Resources
Registration Authority
Central Directory
Documents
Authorization for any network resource
Archive Services
Network Resources
(Agencies, other jurisdictions, external partners)

Transaction:

- execute/sign
- record/log - accounting & record retention mgmt

This is Washington state's framework model.

User
(a meta-directory integrates
directory services which authenticate who, and
access policy services which authorize what):

- Identify,
- Authenticate
- Authorize

Transaction
(a signed or unsigned record committed to by user):

- execute
- record -
  accounting &
  record retention management

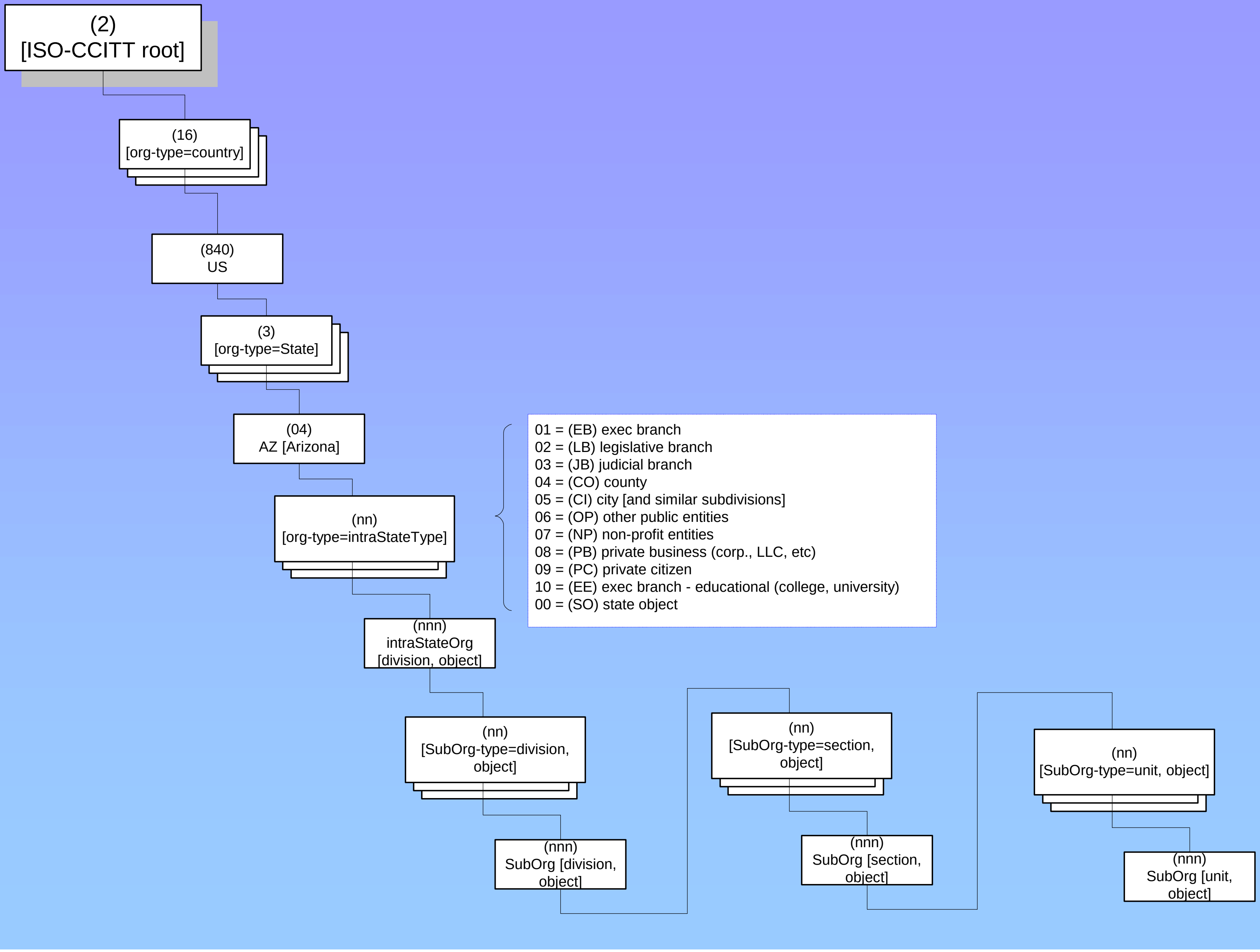
A *unique universal identifier* for a user is
a Distinguished Name (*DN*) - something descriptive but unique.

A *unique universal identifier* for a user role or tool is
an *OID* (a numeric, object identifier)

DN (distinguished names) and OID (object identifiers)

- OID uniquely defines Distinguished Names and Object Identifiers.
- Under the joint-iso-ccitt arc in the registration tree, the US-JRA has registered sub-authorities, including states.
- Arizona's schema builds on the US arc of the registration tree established according to CCITT X.660 Recommendation and ISO/IEC 9834-1 Standard.
- The state arcs are defined by FIPS PUB 5-2.
- The registration sub-authority for Arizona is the Secretary of State
- The root Arizona arc is 2-16-840-3-04
- The first numeric assignment after 2-16-840-3-04 identifies the type of entity within the state.

OID Schema for the State of Arizona



(2)
[ISO-CCITT root]

(16)
[org-type=country]

(840)
US

(3)
[org-type=State]

(04)
AZ [Arizona]

(nn)
[org-type=intraStateType]

01 = (EB) exec branch
02 = (LB) legislative branch
03 = (JB) judicial branch
04 = (CO) county
05 = (CI) city [and similar subdivisions]
06 = (OP) other public entities
07 = (NP) non-profit entities
08 = (PB) private business (corp., LLC, etc)
09 = (PC) private citizen
10 = (EE) exec branch - educational (college, university)
00 = (SO) state object

(nnn)
intraStateOrg
[division, object]

(nn)
[SubOrg-type=division, object]

(nnn)
SubOrg [division, object]

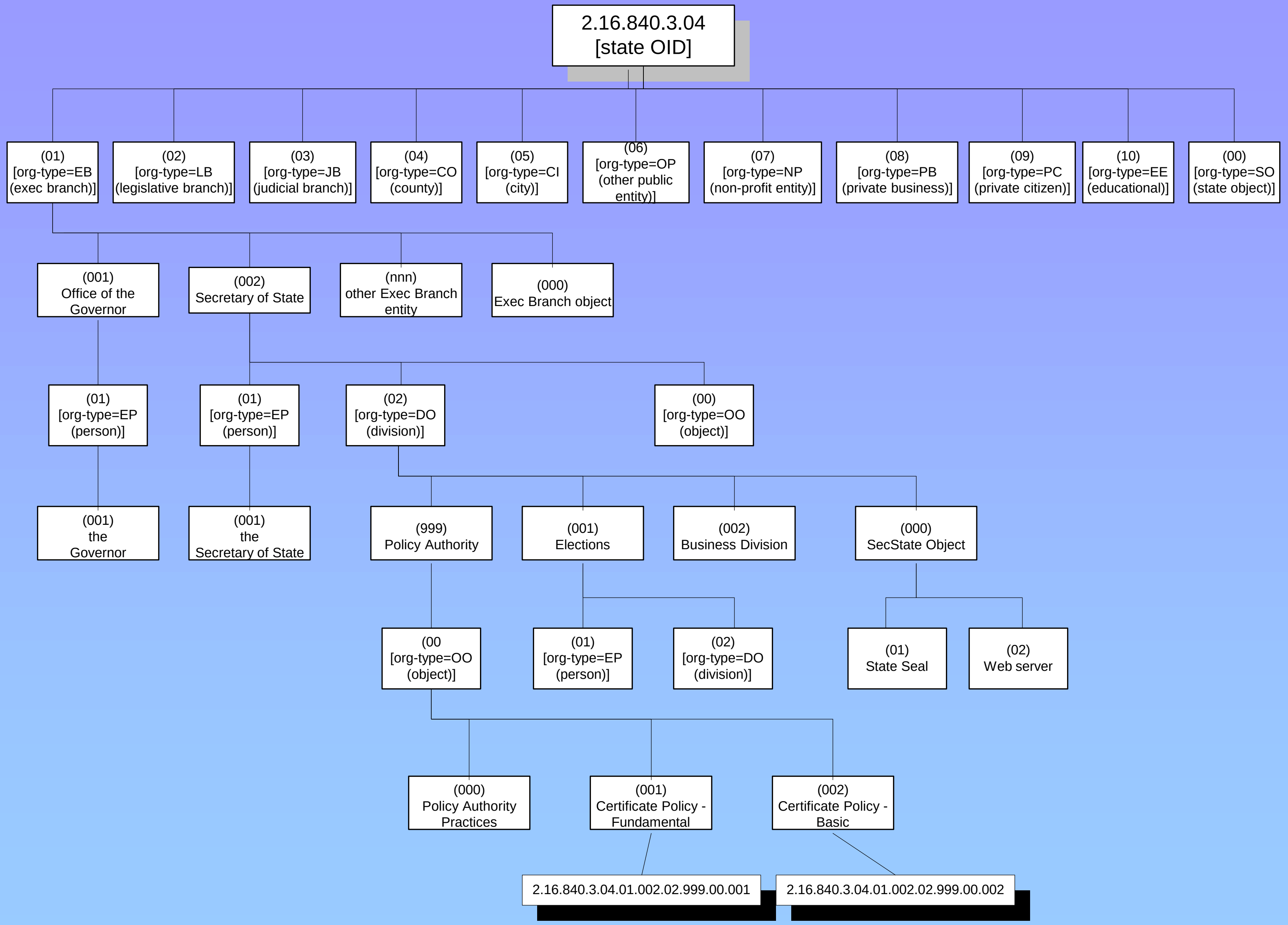
(nn)
[SubOrg-type=section, object]

(nnn)
SubOrg [section, object]

(nn)
[SubOrg-type=unit, object]

(nnn)
SubOrg [unit, object]

OID Schema for the State of Arizona



- 2.16.840.3.04 [state OID]
  - (01) [org-type=EB (exec branch)]
    - (001) Office of the Governor
      - (01) [org-type=EP (person)]
        - (001) the Governor
    - (002) Secretary of State
      - (01) [org-type=EP (person)]
        - (001) the Secretary of State
      - (02) [org-type=DO (division)]
        - (999) Policy Authority
          - (00 [org-type=OO (object)]
            - (000) Policy Authority Practices
            - (001) Certificate Policy - Fundamental
              - 2.16.840.3.04.01.002.02.999.00.001
            - (002) Certificate Policy - Basic
              - 2.16.840.3.04.01.002.02.999.00.002
        - (001) Elections
          - (01) [org-type=EP (person)]
          - (02) [org-type=DO (division)]
        - (002) Business Division
        - (000) SecState Object
          - (01) State Seal
          - (02) Web server
      - (00) [org-type=OO (object)]
    - (nnn) other Exec Branch entity
    - (000) Exec Branch object
  - (02) [org-type=LB (legislative branch)]
  - (03) [org-type=JB (judicial branch)]
  - (04) [org-type=CO (county)]
  - (05) [org-type=CI (city)]
  - (06) [org-type=OP (other public entity)]
  - (07) [org-type=NP (non-profit entity)]
  - (08) [org-type=PB (private business)]
  - (09) [org-type=PC (private citizen)]
  - (10) [org-type=EE (educational)]
  - (00) [org-type=SO (state object)]

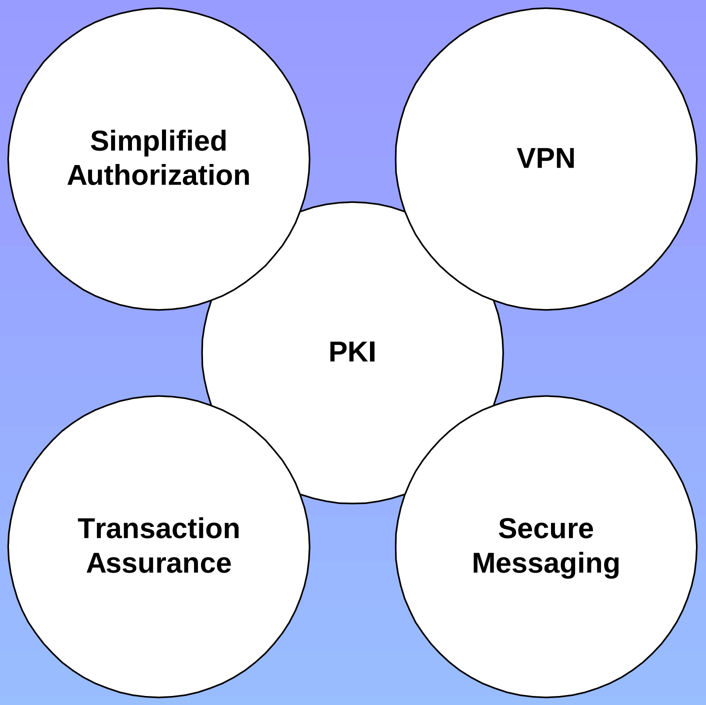
LDAP relies on DN and RDN (Relative Distinguished Name) to define unique entries in the directory schema.

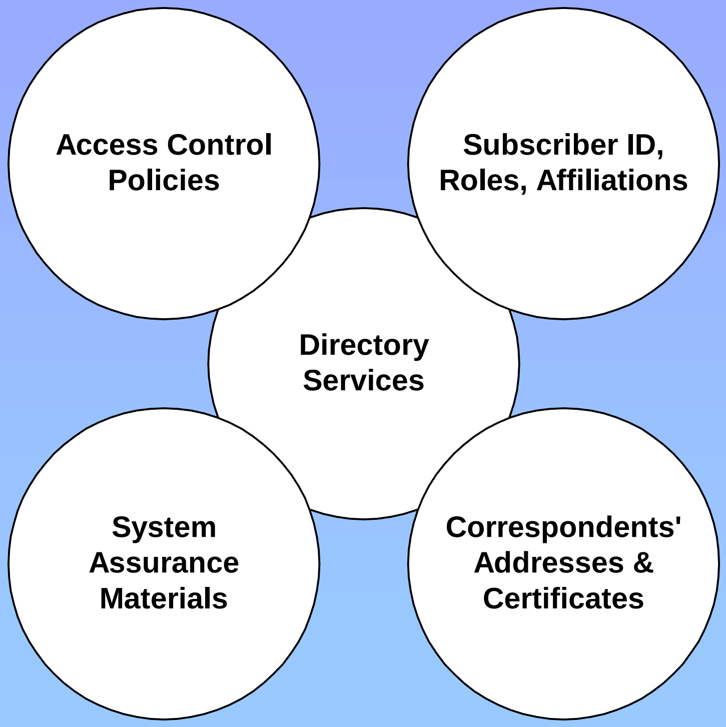
The common elements for mapping between LDAP DN and OID alphanumeric assignments are:

(LDAP element = OID element)

cn=CommonName
sn=Surname
l=LocalityName
st=StateName
o=OrganizationName
ou=OrganizationUnitName
c=CountryName
street=StreetAddress
uid=UserIdentifier

The proposed policy is that
the registered OID alphanumeric arc is the LDAP DN.




Access Control Policies
Subscriber ID, Roles, Affiliations
Directory Services
System Assurance Materials
Correspondents' Addresses & Certificates

Having the registered OID alphanumeric arc as the LDAP DN **bridges** ***PKI and Directory Services.***

Bridging *PKI and Directory Services establishes the framework for the evolution of*:

Directory Enabled Networking (DEN),

Smart Network Devices (DEN/CIM enabled),

Policy Based Authorization (DEN/CIM), and

Electronic Signatures

Though using the same schema and Infrastructure...

Cannot stress enough, the importance for separate key pairs for

identity
signing
encryption

Broad Vision of Scope

Blending managing people and managing transactions

This structure is valuable for

- *Electronic Organization Chart - White pages (finding someone), structured management of access rights and authentication*
- *Facilitates email*
- *directory services - structured management of access rights and authentication*
- *electronic records management, organization, access and authorization*

PKI potential

- No single hierarchy - multiple hierarchies using the same schema
- Multiple PKIs
- Focus on identity, not authorization, certificates
  - authorization a subsequent result

PKI

- Functions:
  - Identity
  - Authentication
  - Directories
  - Authorization
- Lynchpin
  - **LDAP**
- Virtually impossible to predict what will emerge from extremely complex systems; however, PKI will drastically alter the way we learn, work and play in cyberspace.

Looking forward

- Infrastructure not built yet
  - it’s not as common as the driver’s license
  - it’s not as common as the ATM card
- signing processes are this way too.
  - If you had an infrastructure of electronic signatures, digital signatures, would you even be sitting here… or would you have just “filer must evidence state issued ‘electronic’ identity card.”
- but a PKI is what we are building
  - promoting a single hierarchy schema within Arizona
  - acknowledging multiple PKIs
  - Focus on Signature Certificates, but see integration of authorization and environment

PKI is a open system, but with no ‘I’ built, it really is a “Private”

- you issue a certificate to identify a person
- your HR / Domain Users / Email holds that certificate
- your server acts as your public phone book
  - lightweight directory access protocol (LDAP)
- in theory, I go to email someone in your system…
  - I type in your email address
  - my email program tries to access your phone book
  - looks up your name
  - retrieves your public number for me to “dial”
  - thus I can send authenticated / encrypted to you
- problems:
  - my email system does not know how to search your phone book
    - I have to import your key or obtain it some other way
  - Systems have to be “told” who to trust
    - hardly anyone has ldap turned on
  - structure for ldap inconsistent even if it was turned on
    - hopefully I find the right Betsey Bayless
  - Even if I send to you, hopefully your email system is able to handle encrypted email.

The “closed” system of the Community of Interest

- Through CP:
  - we know who the CA is
  - we know who th e RA is
  - we know who the Repository is
- thus the subscriber is brought into network of trust by means of the community
- we may call it open, but infrastructure not there so we need to think of it as closed… and liability of reliance upon signature is defined just that way
- Internal to community, jurisdictions agree to setup resources to interact with

Why a commercial CA?

- Trust hierarchy automatically recognized by most browsers & clients world wide
- Solves liability & security of operating PKI
- Provides significant amount of support resources
- Solves funding pitfalls, if done correctly

Collaborative Statewide Effort

we’re building that infrastructure ;-)